G.D.P.R.
Il Regolamento Europeo sulla protezione dei dati

Regolamento Ue 679/2016

Dalla 675/96 al regolamento Ue

- L.675/96
- D.P.R 318/99 Misure minime di sicurezza
- D.Lgs.196/2003
- Regolamento UE 679/2016 in vigore da maggio 2016. Obbligatorio dal 25 maggio 2018

Schema D.Lgs (21 marzo 2018)

2016 I numeri del Garante

- Riscontro a 4.633 reclami e segnalazioni
- Decisi 277 ricorsi
- 53 Violazioni segnalate all'Autorità Giudiziaria per mancata adozione delle misure di sicurezza
- Contestate 2.339 Sanzioni
- Riscosse sanzioni amministrative per circa 3 milioni e 300 mila euro

Oggetto della tutela

Garanzia che i trattamenti dei dati personali rispettino i diritti e le libertà fondamentali e la dignità dell'interessato (riservatezza, identità personale, diritto alla protezione dei dati)

Cosa intendiamo per dato personale?

Qualsiasi informazione riguardante una persona fisica, identificata o identificabile

Quali dati rendono identificabile una persona fisica?

- Nome, cognome
- Un numero di identificazione
- Dati relativi all'ubicazione
- Identificativo on line
- Uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale

Le categorie di dati personali

- Dati comuni
- Dati sensibili
- Dati giudiziari

- Dati particolari:

  origine razziale ed etnica, opinioni politiche, convinzioni filosofiche o religiose, appartenenza sindacale, dati genetici, dati biometrici, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale

- Dati relativi a condanne penali
- Dati Comuni

Non si possono trattare dati particolari a meno che…

- L'interessato ha prestato il proprio consenso
- Il trattamento sia necessario per assolvere obblighi in materia di diritto del lavoro o sicurezza sociale e protezione sociale
- Il trattamento è effettuato da un'associazione o fondazione e i dati non siano comunicati all'esterno
- Il trattamento riguardi dati resi manifestamente pubblici dall'interessato
- Il trattamento è necessario per finalità di medicina preventiva, del lavoro o valutazione della capacità lavorativa

Ruoli e responsabilità

- Titolare del trattamento

  Persona fisica, giuridica ente o associazione che determina modalità e finalità del trattamento ed i profili della sicurezza

- Responsabile del trattamento

  Soggetto cui il Titolare affida il trattamento dei dati

- Incaricato del trattamento

  Soggetto autorizzato a svolgere operazioni di trattamento che opera sotto il controllo e autorità del Titolare

Informativa Art. 13 Reg. Ue 679/2016

- deve avere forma **concisa, trasparente, intelligibile per l'interessato e facilmente accessibile**; occorre utilizzare un linguaggio **chiaro e semplice**, e per i minori occorre prevedere informative idonee
- L'informativa è data, in linea di principio, per iscritto e preferibilmente in formato elettronico anche se sono ammessi "altri mezzi", quindi può essere fornita anche oralmente

D.Lgs. 196/2003 (in vigore fino al 24 maggio 2018)	Regolamento Ue 679/2016 (dal 25 maggio 2018)
Finalità e modalità di trattamento	
Natura obbligatoria o facoltativa del conferimento dei dati	
	Base giuridica del trattamento
	Se il trattamento si basa sull'art.6, §1 lettera f) , i legittimi interessi perseguiti dal titolare del trattamento o di Terzi
Le conseguenze di un eventuale rifiuto a rispondere	
Soggetti o le categorie di soggetti ai quali i dati possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati, ambito di diffusione dei dati medesimi	Data retention
Diritti dell'art.7	
	Ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione o garanzie appropriate o opportune e i mezzi per ottenere una copia di tali dati o il luogo dove sono stati resi disponibili.
Estremi identificativi del titolare e, se designato del rappresentate nel Territorio dello stato e del responsabile. Quando il titolare ha designato più responsabili è indicato almeno uno di essi, indicando il sito della rete di comunicazione o le modalità attraverso le quali è conoscibile in modo agevole l'elenco dei responsabili.	Identità e dati di contatto del titolare del trattamento
	I dati di contatto del RPD (DPO) ove applicabile

Diritto all'Oblio Art. 17

L'interessato ha diritto di ottenere la cancellazione **senza ingiustificato ritardo** qualora:

- i dati non siano più necessari rispetto alle finalità per le quali sono stati raccolti
- il consenso al trattamento venga revocato
- l' interessato si opponga al trattamento
- i dati siano trattati illecitamente
- i dati debbano essere cancellati per legge

Accountability – Obblighi del titolare

- Responsabilizzazione del titolare finalizzata a conseguire i risultati ovvero la sicurezza dei trattamenti previsti dal regolamento europeo
- Unicamente a responsabili del trattamento che presentino garanzie sufficienti a mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del Regolamento UE 679/2016 e garantisca la tutela dell'interessato

Responsabile Art. 28

- Non ricorre a un altro responsabile senza previa autorizzazione scritta, specifica o generale, del titolare del trattamento.

Nomina del Responsabile

- Disciplinata **da un contratto o da altro atto giuridico** a norma del diritto dell'unione o degli altri Stati membri che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento.

Il contratto prevede in particolare che il responsabile…

- Tratti i dati soltanto su istruzione documentata del titolare
- Garantisca che le persone autorizzate al trattamento si siano impegnate alla riservatezza o abbiano un obbligo legale di riservatezza
- Adotti tutte le misure ai sensi dell'art. 32
- Rispetti le condizioni per ricorrere ad altro responsabile
- Assista il titolare nel rispetto degli obblighi del regolamento
- Su scelta del titolare cancelli o restituisca tutti i dati al termine della prestazione
- Metta a disposizione del titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi del presente articolo (Art. 28)e consenta l'attività di revisione ed ispezione del titolare

Gli incaricati del trattamento

- Chiunque agisca sotto l'autorità del titolare del trattamento o del responsabile o abbia accesso ai dati personali **NON** può trattare tali dati **se non è istruito** in tal senso dal titolare del trattamento.

- Sono nominati per iscritto.

La sicurezza dei dati nel D.Lgs. 196/03

- Misure Idonee

  Art 31

- Misure Minime

  Art 33-34-35

Accountability

- Titolare del trattamento mette in atto misure tecniche e organizzative adeguate per **garantire ed essere in grado di dimostrare,** che il trattamento è effettuato conformemente al presente regolamento.
- Dette misure sono riesaminate e aggiornate qualora necessario

Art.32 Misure di sicurezza

«Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:….»

Art.32 Misure di sicurezza adeguate che comprendono:

- Pseudonimizzazione e la cifratura
- Riservatezza, Integrità e disponibilità dei dati, resilenza dei sistemi e dei servizi
- Capacità di ripristino in caso di incidente fisico o tecnico
- Procedure per testare il ripristino dei dati

Le misure devono Garantire

- Procedura di verifica e valutazione misure di sicurezza
- Analisi dei rischi
- Adesione a Codici di Condotta

Privacy By Design Art. 25 par. 1

- Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione ……

Privacy By Default Art. 25 par. 2

- Il titolare del trattamento mette in atto misure tecniche ed organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati necessari per ogni specifica attività di trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento , il periodo di conservazione, e l'accessibilità.

Registri delle attività di trattamento Art.30

Titolari del trattamento

Responsabili del trattamento

- più di 250 dipendenti
- trattamenti che presentino un rischio per i diritti e le libertà dell'interessato
- categorie particolari di dati (art.9)
- dati giudiziari (art. 10)

Contenuto del registro

- Finalità del trattamento
- Categorie di interessati
- Categorie di destinatari
- Trasferimenti verso paesi terzi
- Tempi per la cancellazione dati
- Misure di sicurezza adottate

Il Garante Italiano cosa raccomanda

La tenuta del registro dei trattamenti non costituisce un adempimento formale bensì ***parte integrante di un sistema di corretta gestione dei dati personali****. Per tale motivo, si invitano tutti i titolari di trattamento e i responsabili, a prescindere dalle dimensioni dell'organizzazione, a compiere i passi necessari per dotarsi di tale registro e, in ogni caso, a compiere un'accurata ricognizione dei trattamenti svolti e delle rispettive caratteristiche – ove già non condotta. I contenuti del registro sono fissati, come detto, nell'art. 30; tuttavia, niente vieta a un titolare o responsabile di inserire ulteriori informazioni se lo si riterrà opportuno proprio nell'ottica della complessiva valutazione di impatto dei trattamenti svolti*

Notificazione violazione dati Art. 33

- Notificare entro le 72 ore dal momento in cui il titolare ne viene a conoscenza
- Se oltre le 72 ore bisogna dare la motivazione del ritardo
  - Natura della violazione
  - Ove possibile, categorie e numero di interessati e di registrazioni di dati personali coinvolti
  - Nome e dati di contatto del responsabile della protezione dei dati o altro soggetto di riferimento
  - Descrizione probabili conseguenze della violazione
  - Descrizione misure adottate o da adottare per porre rimedio alla violazione e attenuarne effetti negativi

L’obbligo della comunicazione all’interessato viene meno se:

- Erano state applicate ai dati oggetto della violazione misure di sicurezza adeguate, in particolare quelle idonee a renderli incomprensibili (es, la cifratura).
- Il titolare del trattamento ha adottato in seguito alla violazione misure idonee ad evitare il sopraggiungere di un rischio elevato per i diritti e le libertà personali.
- Tale comunicazione richiederebbe sforzi sproporzionati. In tal caso si dovrà fare una comunicazione pubblica.

Valutazione d'impatto sulla protezione dei dati Art. 35

- Il trattamento può presentare un rischio elevato per i diritti e le libertà delle persone fisiche
- Valutazione sistematica e globale di aspetti personali relative a persone fisiche (*profilazione*)
- Trattamento su larga scala di dati personali particolari (art. 9 e art.10)
- Sorveglianza sistematica su larga scala di una zona accessibile al pubblico

La consultazione preventiva Art. 36

Quando?

- Prima di procedere al trattamento
- Se la valutazione d'impatto indica che il trattamento presenta un **rischio elevato** ed il Titolare deve quindi adottare misure idonee ad attenuare tale rischi

Responsabile della protezione dei dati (DPO) Art. 37

Designato in funzione:

- delle qualità professionali
- della capacità di assolvere ai compiti indicati di cui dall'art. 39

Può essere:

- Un dipendente del titolare o del responsabile (non in conflitto di interessi)

Oppure

- Può svolgere i suoi compiti sulla base di un contratto di servizi

Responsabile della protezione dei dati (DPO) Art. 37

Il ruolo di responsabile della protezione dei dati personali è compatibile con altri incarichi?

Si, a condizione che non sia in conflitto di interessi. In tale prospettiva, appare preferibile evitare di assegnare il ruolo di responsabile della protezione dei dati personali a soggetti con incarichi di alta direzione (amministratore delegato; membro del consiglio di amministrazione; direttore generale; ecc.), ovvero nell'ambito di strutture aventi potere decisionale in ordine alle finalità e alle modalità del trattamento (direzione risorse umane, direzione marketing, direzione finanziaria, responsabile IT ecc.). Da valutare, in assenza di conflitti di interesse e in base al contesto di riferimento, l'eventuale assegnazione di tale incarico ai responsabili delle funzioni di staff (ad esempio, il responsabile della funzione legale).

Quando è obbligatorio

a) se il trattamento è svolto da un'autorità pubblica o da un organismo pubblico;

b) se le attività principali del titolare o del responsabile consistono in trattamenti che richiedono il monitoraggio regolare e sistematico di interessati su larga scala; oppure

c) se le attività principali del titolare o del responsabile consistono nel trattamento su larga scala di categorie particolari di dati o di dati personali relativi a condanne penali e reati.

Quando è obbligatorio (Sito Garante)

«Ricorrendo i suddetti presupposti sono tenuti alla nomina, a titolo esemplificativo e non esaustivo: istituti di credito; imprese assicurative; sistemi di informazione creditizia; società finanziarie; società di informazioni commerciali; società di revisione contabile; società di recupero crediti; istituti di vigilanza; partiti e movimenti politici; sindacati; caf e patronati; società operanti nel settore delle "utilities" (telecomunicazioni, distribuzione di energia elettrica o gas); imprese di somministrazione di lavoro e ricerca del personale; società operanti nel settore della cura della salute, della prevenzione/diagnostica sanitaria quali ospedali privati, terme, laboratori di analisi mediche e centri di riabilitazione; società di call center; società che forniscono servizi informatici; società che erogano servizi televisivi a pagamento.»

Quando non è obbligatorio (Sito Garante)

«Nei casi diversi da quelli previsti dall'art. 37, par. 1, lett. b) e c), …ad esempio, in relazione a trattamenti effettuati da liberi professionisti operanti in forma individuale; agenti, rappresentanti e mediatori operanti non su larga scala; imprese individuali o familiari; piccole e medie imprese, con riferimento ai trattamenti dei dati personali connessi alla gestione corrente dei rapporti con fornitori e dipendenti: v. anche considerando 97 del Regolamento, in relazione alla definizione di attività "accessoria"»

Compiti del DPO

- Consulenza sugli obblighi derivanti dal regolamento
- Sorvegliare l'osservanza del Regolamento
- Fornire pareri sulla PIA e sorvegliare lo svolgimento
- Fungere da contatto con l'autorità di controllo

Sanzioni – Gli stati membri

- Stabiliscono le **norme relative alle sanzioni** per le violazioni del presente regolamento in particolare per le violazioni non soggette a sanzioni amministrative pecuniarie a norma dell'art. 83, e adottano tutti i provvedimenti necessari per assicurarne l'applicazione.
- Tali sanzioni devono essere effettive, proporzionate e dissuasive

Sanzioni

Sanzioni pecuniarie sino a 20.000.000,00 di euro o, per le imprese, fino al 4% del fatturato mondiale annuo

- Violazione dei principi del trattamento, comprese le condizioni di consenso
- Diritti degli interessati
- Trasferimento verso un paese terzo
- Qualsiasi obbligo ai sensi delle legislazioni degli stati membri

Sanzioni

Sanzioni pecuniarie sino a 10.000.000,00 di euro 0, per le imprese, fino al 2% del fatturato mondiale annuo

- Violazione degli obblighi del titolare del trattamento
- Obblighi dell'organismo di certificazione
- Obblighi dell'organismo di controllo

Art. 80 Regolamento UE

L'interessato ha il diritto di dare mandato a un organismo, un'organizzazione o un'associazione senza scopo di lucro, che siano debitamente costituiti secondo il diritto di uno Stato membro, i cui obiettivi statutari siano di pubblico interesse e che siano attivi nel settore della protezione dei diritti e delle libertà degli interessati con riguardo alla protezione dei dati personali, di proporre il reclamo per suo conto e di esercitare per suo conto i diritti di cui agli articoli 77, 78 e 79 nonché, se previsto dal diritto degli Stati membri, il diritto di ottenere il risarcimento di cui all'articolo 82.

Art. 82 Regolamento UE

- Chiunque subisca un danno materiale o immateriale causato da una violazione del presente regolamento ha il diritto di ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento.
- Un titolare del trattamento coinvolto nel trattamento risponde per il danno cagionato dal suo trattamento che violi il presente regolamento. Un responsabile del trattamento risponde per il danno causato dal trattamento solo se non ha adempiuto gli obblighi del presente regolamento specificatamente diretti ai responsabili del trattamento o ha agito in modo difforme o contrario rispetto alle legittime istruzioni del titolare del trattamento.

Ma alla fine cosa devo fare?

- **Mappatura** dei dati personali trattati per decidere come procedere: quali dati, chi li gestisce, come….ecc.
- **Aggiornare le informative** e relativi **consensi** se serve.
- Verificare e implementare la «**Data Protection**» per le richieste, DPIA, data breach, misure adeguate, istruzioni incaricati, profili di autorizzazione, ecc..
- Se siete **Responsabili esterni** bisogna adeguare anche la contrattualistica (Art 28)
- Codici di condotta e/o meccanismi di certificazione